Groupes opérant sur un ensemble.
Groupes de SYLOW

(Dany-Jack MERCIER, 1979)

Définition _ Équation des classes.

On dit qu'un groupe G opère sur un ensemble E, à gauche, si ∃ loi externe

$$G \times E \longrightarrow E$$
$$(g, x) \longmapsto g.x$$

qui vérifie : 1) $g.(g'.x) = (gg').x \quad \forall g, g' \in G \ \forall x \in E$

2) $e.x = x \quad \forall x \in E$

Th | L'ensemble E est un G-ensemble si et seulement si G est homomorphe au groupe S(E)

NB : S(E) est le groupe symétrique de E, c.à.d le groupe de toutes les permutations de E dans E, muni de o.
L'homomorphisme $T : G \to S(E)$ annoncé n'est autre que $T_g(x) = g.x$.

<u>Définitions</u> :

a) G opère fidèlement sur E si $T : G \to S(E)$ est injectif,
c.à.d si $gx = x \ \forall x \in E \Rightarrow g = e$

b) $G_x = \{ y \in E / \exists g \in G \quad y = g.x \}$ = orbite de x pour le groupe G.

c) $H_x = \{ g \in G / gx = x \}$ est un sous-groupe de G. C'est le sous-groupe d'isotropie, ou "stabilisateur" de x dans G.

Th | Soit Ω une orbite pour G. Si x et y sont éléments de Ω, alors les groupes d'isotropie H_x et H_y sont conjugués dans G.

On remarque que la relation dans E : $x \sim y \Leftrightarrow \exists g \in G \quad y = gx$ est une relation d'équivalence, et que les classes de ∼ ne sont autres que les orbites dans E :
plus précisément : $\dot{x}_{(\sim)} = G_x$
Les orbites de E forment donc une partition de E.
Montrons le théorème :

$$x, y \in \Omega = G_y \Leftrightarrow \exists \sigma \in G \quad x = \sigma.y$$

Donc :

$$h \in H_x \Leftrightarrow h.x = x \Leftrightarrow (h\sigma).y = \sigma.y \Leftrightarrow (\sigma^{-1}h\sigma).y = y$$
$$\Leftrightarrow \sigma^{-1}h\sigma \in H_y \Leftrightarrow h \in \sigma H_y \sigma^{-1}$$

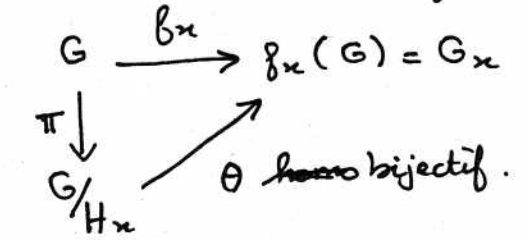
d'où $H_x = \sigma H_y \sigma^{-1}$, ce qui signifie que le sous-groupe H_x est le conjugué de H_y.
CQFD

Considérons $f_x : G \longrightarrow E$ (x fixé)
$g \mapsto g\cdot x$

f_x se factorise canoniquement puisque :

$$f_x(g_1) = f_x(g_2) \Leftrightarrow g_1\cdot x = g_2\, x \Leftrightarrow g_2^{-1} g_1 \cdot x = x \Leftrightarrow g_2^{-1} g_1 \in H_x$$

Ainsi, le diagramme suivant est commutatif :



classes à gauche suivant le sous-groupe d'isotopie H_x.

Ainsi, si G est fini : $\# G_x = \# G/H_x = \dfrac{\# G}{\# H_x}$

$$\boxed{\# G_x = \frac{\# G}{\# H_x}}$$

<u>Équation des classes</u> :

Si l'ensemble E est fini, chaque orbite est un ensemble fini. Si $E' \subset E$, E' ne contient qu'un élément et un seul de chaque orbite, alors, eu égard à la partition réalisée par la relation $\sim$ dans E :

$$\boxed{\# E = \sum_{x \in E'} \# G_x = \sum_{x\in E'} \frac{\# G}{\# H_x}} \quad \text{(équation des classes)}$$

<u>Exemple</u> : G groupe fini. $\varphi : G \longrightarrow \mathrm{Int}(G) \subset S(G)$
$g \longmapsto \varphi_g \;/\; \varphi_g(x) = g x g^{-1}$

φ est un épimorphisme de groupes.
C'est donc un G-ensemble pour la loi dite de conjugaison : $G\times G \to G$
$(g, x) \mapsto g x g^{-1}$

H_x = stabilisateur de x = $\{ g \in G \;/\; gx = xg \}$

Si $z \in Z(G)$ $H_z = G$ et réciproquement. Donc $\# G_z = 1$

L'équation des classes implique : $\# G = \sum_{x\in Z(G)} \# G_x + \sum_{x \in A} \# G_x$

(A = ensemble des éléments de G tel que 2 éléments quelconques de A ne sont pas conjugués). Ainsi :

$$\boxed{\# G = \# Z(G) + \sum_{x\in A} \# G_x}$$

<u>exercice</u>: $p \in \mathcal{P}$, G groupe d'ordre p^k. Alors $Z(G)$ n'est pas trivial.
[Sol : Pour $x \notin Z(G)$, Card G_x divise proprement p^k donc est une puissance de p.
On a $\# Z(G) = \# G - \sum_{x \notin Z(G)} \# G_x \Rightarrow \# Z(G) \equiv 0\ [p] \Rightarrow Z(G)$ non trivial]
(Théorème de Burnside)

Groupes primaires, groupes de Sylow   1°/ **Définitions et premières propriétés.**

Th 1 | Tout groupe fini commutatif contient un élément d'ordre $p \in \mathcal{P}$ si $p | \#$

Th 2 | Soit G un groupe fini d'ordre n, et $p \in \mathcal{P}$ / $p^k | n$.
Alors G contient un sous-groupe d'ordre p^k

preuve : le théorème est trivial si $n = p^k$.
On raisonne par récurrence sur n en supposant le théorème vrai pour tous les group[es] d'ordre $n' < n$.
G est un G-ensemble pour la loi de conjugaison $(g, x) \longmapsto g x g^{-1}$.
De 2 choses l'une :

a) $\exists x \notin Z(G) / \# G_x \not\equiv 0 \, [p]$. Alors $n = \# H_x \cdot \# G_x$
p, premier, est premier avec tout nombre qu'il ne divise pas. Donc $\Delta(p^k, \# G_x) =$ [1]
et le théorème de Gauss donne : $p^k | \# H_x$. H_x, stabilisateur de x, est un sous-groupe de G d'ordre $\# H_x = \frac{n}{\# G_x} < n$ puisque $\# G_x > 1$.
D'après l'hyp. de récurrence :

H_x possède un sous-groupe d'ordre p^k

b) $\forall x \notin Z(G) / \# G_x \equiv 0 \, [p]$.
L'équation des classes donne :

$$\# Z(G) = n - \sum_{x \in A} \# G_x \equiv 0 \quad [p]$$

Le centre $Z(G)$ n'est pas trivial. Comme $p | \# Z(G)$, il existe selon le th. 1 un élément $a \in Z(G)$ d'ordre p. Le groupe $\langle a \rangle = H$ est d'ordre p. Il est distingué dans G, puisque $H \subset Z(G)$.

$p^k | n \Rightarrow p^{k-1} | \# (G/_H)$
D'après l'hypothèse de récurrence, $\exists K' \subset G/_H$ K' sous-groupe d'ordre p^{k-1}
Soit $\pi : G \to G/_H$ et $K = \pi^{-1}(K')$. $K \supset H$ et $\pi|_K : K \longrightarrow K'$
donc $K/_H \simeq K' \Rightarrow \# K = p^k$

$$\begin{array}{ccc} K & \longrightarrow & K' \\ \downarrow & \nearrow & \\ K/_H & \sim \text{groupes} & \end{array}$$

CQFD

Def | Soit p un nombre premier.
- Un p-groupe (ou groupe p-primaire) est un groupe fini d'ordre p^α
- Si $H \subset G$, H est un p-groupe, on dira que c'est un p-sous-groupe de G.
- Si $H \subset G$ est un p-sous-groupe de G de cardinal p^n où p^n est la plus grande puissance de p qui divise $\# G$, alors H sera dit "un p sous-groupe de Sylow.

(NB : $H \subset G$ est un p sous-groupe de Sylow ssi c'est un p-sous-groupe maximal

Co | Soit G un groupe fini et $p \in \mathcal{P}$ $p | \# G$. Alors il existe un p-sous-groupe de Sylow de G.

Exercices :

① Tout conjugué d'un p sous-groupe de Sylow est encore un p sous-groupe de Sylow

[$H \subset G$ $\#H = p^n$ où $\#G = n = p^n m$ $\Delta(p,m) = 1$. $H' = gHg^{-1} = \varphi_g(H)$ où $\varphi_g(x) = gxg^{-1}$ est un automorphisme intérieur. φ_g est bijectif, donc conserve le cardinal].

② Soit G un groupe abélien fini de cardinal n.

$$\exists m \in \mathbb{N}^* \ / \ \forall g \in G \quad mg = 0 \quad \Rightarrow \exists k \in \mathbb{N} \quad n \mid m^k$$

[Par récurrence sur m. Soit $g \in G$, $g \neq 0$ et $H = \langle g \rangle$. $\# G/H < n$
G/H est un groupe, et $m\dot{g} = \dot{0}$ $\forall \dot{g} \in G/H$. D'après l'hypothèse de récurrence, $\# G/H \mid m^k$ or $\# G/H = \frac{\#G}{\#H} = \frac{n}{\#H}$ et $\#H \mid m$

d'où $\frac{n}{\#H} \mid m^k \Leftrightarrow m^k = \lambda \frac{n}{\#H}$ et $m = \mu \# H$ d'où $m^{k+1} = \mu \lambda n \Leftrightarrow n \mid m^{k+1}$

Th 3 | Si P est un p sous-groupe de Sylow d'un groupe fini, alors tout p-sous-groupe de N(P) est contenu dans P.

(Rappel : $N(H) = \{ g \in G \ / \ gHg^{-1} = H \}$)
preuve : Soit R un p sous-groupe contenu dans N(P). Comme $P \triangleleft N(P)$ et $R \subset N(P)$
$R/_{P \cap R} \simeq PR/_P$. Or $\#(R/_{P\cap R}) = p^\alpha \Rightarrow \# PR/_P = p^\alpha$ et a fortiori $\#(PR) = p^\beta$
P.R est donc un p-groupe de G, et il contient P. Mais P est un p sous-groupe de Sylow, donc maximal parmi les p-sous-groupes, d'où $PR = P \Rightarrow R \subset P$

Th 4 | Soit H un sous-groupe du groupe fini G
Alors :
H = p-sous-groupe de Sylow $\Longleftrightarrow$ H = maximal dans l'ensemble des p-groupes de G ordonné par l'inclusion.

($\Rightarrow$) $\#H = p^k$ où $n = p^k m$ $\Delta(m,p) = 1$.
Soit K un p-sousgroupe de G contenant H. $\#K = p^\alpha$
$H \subset K \Rightarrow k \leq \alpha$
K sous-groupe de G $\Rightarrow \alpha \leq k$ $\Big\} \Rightarrow \#K = p^k = \#H \Rightarrow H = K$
Donc H est maximal.

($\Leftarrow$) notons $\#H = p^\alpha$. d'autre part il existe $K \subset G$ / $\#K = p^k$ où $n = p^k . m'$ $(\Delta(m', p) = 1)$. considérons $\Lambda = \{ x \in G \ / \ x^{p^k} = e \}$. alors on rem. que Λ est un p-sous-groupe de G, et que $H \subset \Lambda$. H étant maximal, on a donc $H = \Lambda$ or $K \subset \Lambda = H$ d'où (à cause des cardinaux), $K = H$, H est donc un p-sous-groupe de Sylow.

2°/ Théorème de Cauchy

On généralise le Th 1 précédent :

Th | (de Cauchy) Soit G un groupe fini d'ordre n et p un diviseur premier de n. G possède un élément d'ordre p.

preuve : récurrence sur $\# G = n$. Si $n = 2$, $G = \mathbb{Z}/2\mathbb{Z}$ et l'assertion est vraie.
Supposons la démontrée pour tout $m < n$. Soit $p | n$, $p \in \mathcal{P}$.
Si $G = Z(G)$, le résultat est vrai (cf. Th 1)
Supposons $G \neq Z(G)$. De 2 choses l'une :

a) $\exists x \in G \setminus Z(G)$ tel que $p \mid \# H_x$

(Ici, H_x = stabilisateur de x pour la conjugaison $= \{g \in G \, / \, g^{-1} x g = x\}$ on le nomme aussi le centralisateur de G.)
Mais $x \notin Z(G) \Rightarrow H_x \subsetneq G \Rightarrow \# H_x < \# G$ et d'après l'hypothèse de récurrence, il existe un élément d'ordre p dans H_x, donc dans G.

b) $\forall x \in G \setminus Z(G)$, $p \nmid \# H_x$

Mais $p \in \mathcal{P}$ divise $n = \# G = \# G/_{H_x} \cdot \# H_x$ et $p \nmid \# H_x$, donc $p \mid \# G/_{H_x}$ pour tout $x \notin Z(G)$
D'après l'équation des classes :

$$\# G - \sum_{x \in A} \# G/_{H_x} = \# Z(G)$$

donc $p \mid \# Z(G)$ et $Z(G)$ est commutatif ! Le Th 1 nous donne l'existence d'un élément d'ordre p dans $Z(G)$, donc dans G.
CQFD

Exemple : Dans $\mathcal{S}_4$, il y a un élément d'ordre 2 et un d'ordre 3.
En effet : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Ce théorème permet de donner une équivalence précieuse entre définitions :

Pro | Soit G un groupe fini. Alors :
$$\# G = p^k \iff \{\forall x \in G \ \exists \alpha \in \mathbb{N} \quad p^\alpha x = 0\}$$

(NB : d'où une autre définition d'un p-groupe, si G est un groupe fini. Dans le cas où G est infini, G est dit p-groupe si $\forall x \in G \ \exists \alpha \, / \, \omega(x) = p^\alpha$, et la définition de "droite" s'avère plus généralisable ...)

- Si $\# G = p^k$ $\forall x \in G$ $\langle x \rangle \subset G \Rightarrow \omega(x) = p^\alpha$ (Th. Lagrange)
- Inversement, si $\forall x \in G$ $\exists \alpha$ $p^\alpha x = 0$, supposons que $q \in \mathcal{P}$ $q \mid \#$
D'après le théorème de Cauchy ci-dessus, G possède un élément d'ordre q. Donc $\exists \alpha \, / \, q = p^\alpha$ et $q \in \mathcal{P} \Rightarrow \alpha = 1$. Ainsi $q = p \Rightarrow \# G = p^k$

3°/ Dénombrement des p-groupes de Sylow

Th 5 | Deux p-sous-groupes de Sylow d'un groupe fini G sont conjugués dans G.
Le nombre de p-sous-groupes de Sylow de G est de la forme $1 + kp$

(NB : on sait déjà que si H est un p-sous-groupe de Sylow, alors tous les conjugués de H sont aussi des p-sous-groupes de Sylow)

Deux parties :

1° partie : On montre que $\# \mathcal{O} = r \equiv 1 [p]$

G opère sur $\mathcal{H}$ ensemble des sous-groupes de G, par conjugaison : $G \times \mathcal{H} \longrightarrow \mathcal{H}$, $g, H \longmapsto gHg^{-1}$

P = sgroupe de Sylow

$N(P) = G_P = \{g \in G \,/\, gPg^{-1} = P\}$ = groupe d'isotropie, ou stabilisateur, de P.
(NB : ici, il est égal au normalisateur de P)

On désigne par $\mathcal{O}$ l'orbite de P. On a : $\# \mathcal{O} = r = \#G / \#N(P)$

P opère sur $\mathcal{O}$ par conjugaison : $P \times \mathcal{O} \longrightarrow \mathcal{O}$, $h, H \longmapsto hHh^{-1}$

Soit $\mathcal{U}$ l'orbite de P sous cette action.

$$\mathcal{U} = \{O \in \mathcal{O} \,/\, \exists h \ hPh^{-1} = O\} = \{P\}$$

Ainsi $\# \mathcal{U} = 1$.

Soit $\mathcal{U}_i$ = orbite de $P_i \in \mathcal{O}$, pour $P_i \neq P$.

Si $\# \mathcal{U}_i = 1 \Rightarrow hP_ih^{-1} = P_i \quad \forall h \in P \Rightarrow P \subset N(P_i)$ et d'après le théorème 3 : $P \subset P_i$ (car P = p-sous-groupe).

Comme P est maximal dans l'ensemble des p-groupes $P \subset P_i \Rightarrow P = P_i$, ce qui est absurde.

Donc $P_i \neq P \Rightarrow \# \mathcal{U}_i \neq 1$. L'équation des classes donne :

$$\# \mathcal{O} = r = 1 + \sum_{P_i \neq P} \# \mathcal{U}_i$$

Notons H_i le stabilisateur de P_i sous l'action de P opérant sur $\mathcal{O}$ par conjugaison :

$$\# \mathcal{U}_i = \#P_i / \#H_i \Rightarrow \#P_i = (\#\mathcal{U}_i)(\#H_i) \Rightarrow \#\mathcal{U}_i \equiv 0 \ [p]$$
($\#\mathcal{U}_i \neq 1$ et P_i = p-s.groupe de Sylow)

d'où $r \equiv 1 \ [p]$. $(r = \#\mathcal{O})$ (1)

2° partie : Tous les p-sgroupes de Sylow sont dans $\mathcal{O}$.

Soit Q un p-sous-groupe de Sylow non conjugué à P. Cela revient à dire que $Q \notin \mathcal{O}$

Q opère par conjugaison sur $\mathcal{O}$ $\quad Q \times \mathcal{O} \longrightarrow \mathcal{O}$, $(q, O) \longmapsto qOq^{-1}$

Si $\mathcal{V}_i$ = orbite de $P_i \in \mathcal{O}$, alors $\forall P_i \in \mathcal{O}$: $\# \mathcal{V}_i \neq 1$

[$\# \mathcal{V}_i = 1 \Rightarrow \forall q \in Q \ \ qP_iq^{-1} = P_i \Rightarrow Q \subset N(P_i) \Rightarrow Q \subset P_i$ (th3)
donc $Q = P_i$ (cf. Q maximal)
Donc $\# \mathcal{V}_i \neq 1$]

L'équation des classes est ici : $\# \mathcal{O} = \sum \# \mathcal{V}_i \quad$ où $\# \mathcal{V}_i = \dfrac{\# Q}{\#(\text{stabilisateur de } P_i)}$

$\# \mathcal{V}_i \neq 1 \Leftrightarrow \# \mathcal{V}_i > 1 \Rightarrow \# Q > \#(\text{stabilisateur de } P_i)$.

Comme $\# Q = p^n$ et que (stabilisateur de P_i) $\subset Q$ est de cardinal p^α, et comme $p^n > p^\alpha$, on en déduit que $\# \mathcal{V}_i \equiv 0 \ [p]$.

Donc $\# \mathcal{O} = \sum \# \mathcal{V}_i \equiv 0 \ [p]$ ce qui est absurde selon (1) !

Conclusion : Q = p sous-groupe de Sylow $\Rightarrow Q \in \mathcal{O}$ (orbite de P)
et $\# \mathcal{O} = r \equiv 1 \ [p]$.

4%

Pro | Soit G un p-groupe.
1) Alors $Z(G) \neq \{e\}$
2) G est résoluble.

preuve : 1) On considère l'Équation des classes pour l'opération de conjugaison :

$G \times G \to G$

$(g, x) \mapsto gxg^{-1}$ $\qquad \# G = \# Z(G) + \sum_{x \in A} \frac{\# G}{\# H_x}$ ($\# H_x$: $\# G_x$)

Comme $\# G = p^n$, $G_x \subset G \Rightarrow \# G_x \mid p^n$

et $\# G_x \neq p^n$ (sinon $G_x = G$ et $Z(G) = G$!) Donc $\# Z(G) \equiv 0 \; [p]$. (1)

2) <u>G est résoluble.</u>

Récurrence sur $\# G$.

- vrai pour $\# G = 2$ car $G = \mathbb{Z}/2\mathbb{Z}$ résoluble car commutatif.
- $Z(G) \subset G$ est un sgroupe de G et $\# G/Z(G) < \# G$ d'après (1)

Alors :

$$G/Z(G) = G'_0 \supset G'_1 \supset \ldots \supset G'_n = \{e\} \qquad (2)$$
où $G'_{k+1} \triangleleft G'_k$ et G'_k / G'_{k+1} commutatif

Notons $\pi : G \to G/Z(G)$. On pose $G_i = \pi^{-1}(G'_i)$. On sait que π est une bijection croissante de l'ensemble des sous-groupes contenant $Z(G)$ sur l'ensemble des sous-groupes de $G/Z(G)$. Ainsi (2) $\Rightarrow$

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \pi^{-1}(e) = Z(G)$$

et $\begin{cases} \cdot \; G_{k+1} \triangleleft G_k \\ \cdot \; G_k / G_{k+1} \simeq G'_k / G'_{k+1} \end{cases}$

CQFD

[NB : $\cdot \; \forall x \in G_k \; \forall g \in G_{k+1}, \; \dot{\overline{xgx^{-1}}} \in G'_{k+1} \Rightarrow \dot{\overline{xgx^{-1}}} = \dot{g}' \quad g' \in G_{k+1}$
c.à.d $xgx^{-1}g'^{-1} \in Z(G) \subset G_{k+1} \Rightarrow xgx^{-1} \in G_{k+1}$.

- Considérons $\pi : G_i / G_{i+1} \longrightarrow G'_i / G'_{i+1}$. C'est un isomorphisme.

$\dot{x} \longmapsto \overline{\pi(x)}$

* π est bien définie car $\dot{x} = \dot{y} \Leftrightarrow xy^{-1} \in G_{i+1} \Rightarrow \pi(x)\pi(y)^{-1} \in G'_{i+1} \Leftrightarrow \overline{\pi(x)} = \overline{\pi(y)}$
* π surjective.
* π injective : car $\begin{cases} \overline{\pi(x)} = \bar{0} \Leftrightarrow \pi(x) \in G'_{i+1} \Leftrightarrow x \in G_{i+1} \\ x \in G_i \end{cases} \Rightarrow \dot{x} = \dot{0}$.]